International Journal of Research - GRANTHAALAYAH
November 2025 13(11)
www.granthaalayah.com

Original Article

ESSENTIALS OF NUMBER THEORY FOR CRYPTOGRAPHY

Sujit K. Bose [1*]
[1] S.N. Bose National Centre for Basic Sciences, Salt Lake City, Kolkata 700106, India

ABSTRACT

In the communication era, secure transmission of digital data through networks of communication channels and their storage is carried out by encrypting the data. It transpires that the encryption methods heavily depend on The Theory of Numbers - a fancied topic of Higher Algebra. The discreteness inherent in this algebra employs special constructs, setting it apart from other topics of the subject. Its logical development requires careful understanding of the theory. On the other hand, Cryptography as a subject freely employs the concepts and methods of Number Theory, and a number of books have appeared on the subject. The reading of these texts however is not smooth for readers not conversant with the certain specialities of Number Theory. This survey in simple terms, is a compendium of these specialities that may ease the study of Cryptography.

Keywords: Cryptography, Number Theory, Primes, Congruence, Elliptic Curves

INTRODUCTION

Natural numbers and in general the entire set of integers, has been a subject of study for millennia, unveiling a host of algebraic properties possessing bewilderingly elegant structures. The quest for finding these properties shrouded in right earnest began with the notings of Pierre de Fermat (CE 1601-1665), Euler (CE 1707-1783), Gauss (CE 1777-1855), and numerous other famous mathematicians, continuing to the present era. The subject however remained a special topic in text books of Higher Algebra, such as those by Chrystal (1906) and Bernard and Child (1965) in English language, but the topic gained limelight with the appearance of the tome by Hardy and Wright (1938)followed by a number of other books. Until the mid-nineteen seventies, the subject remained a fancied subject of puree. mathematicians devoid of any practical application.

The invention of the digital computer heralded first as a number crunching machine and then as a coded text editor post 1975 followed by their communication from one computer to another over long distances in a secure manner avoiding any corruption, led to discovering the means of encryption. The subject of Cryptography thus came in to being at that juncture, and as a tool of encryption of stored and transmitted data, the vast knowledge of Number Theory at last found a very effective application; the essential reason for this development being discreteness of digital data.

At present the development of the cryptographic methods are treated in several books. Their presentations can be broadly categorised in to two types. Firstly, excellent introductory texts on Cryptography are those by Paar and Pelzl (2010), McAndrew (2011), Hoffstein et al. (2008). and by Buchmann (2002). These books begin with introductory Number Theory, freely employing its special tools, in order to develop various cryptographic methods, many of which employed in practice. Yet the reading such texts is exhausting because of the special features of the Number Theoretic Algebra. The second category of books are on Number Theory,

*Corresponding Author:
Email address: Sujit K. Bose (sujitkbose1@gmail.com)

Received: 06 October 2025; **Accepted:** 23 November 2025; **Published** 16 December 2025
DOI: 10.29121/granthaalayah.v13.i11.2025.6517
Page Number: 106-125
Journal Title: International Journal of Research -GRANTHAALAYAH
Journal Abbreviation: Int. J. Res. Granthaalayah
Online ISSN: 2350-0530, **Print ISSN:** 2394-3629
Publisher: Granthaalayah Publications and Printers, India
Conflict of Interests: The authors declare that they have no competing interests.
Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Authors' Contributions: Each author made an equal contribution to the conception and design of the study. All authors have reviewed and approved the final version of the manuscript for publication.
Transparency: The authors affirm that this manuscript presents an honest, accurate, and transparent account of the study. All essential aspects have been included, and any deviations from the original study plan have been clearly explained. The writing process strictly adhered to established ethical standards.

succinctly presenting some Cryptographic methods. Notable among these texts are those by Rosen (2005) and by Niven et al. (1991). The array of the elegant Number Theoretic results are then applied to special Cryptographic methods. As an aid for easily following the literature on Cryptography, the present survey presents the essentials of Number Theory that may be useful as as a ready reference, The details of this presentation is kept as simple as possible as the goal is to understand the cryptographic methods.

The Theory of Numbers exclusively deals with *whole numbers or integers* consisting of the *natural numbers* $1, 2, 3, 4, \cdots\cdots$, the number 0, and the negative integers $\cdots\cdots, -4, -3, -2, -1$. These numbers form the integer set

$$Z = \{\ldots\ldots\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\ldots\ldots\ldots\ldots\}$$

The theory develops the special properties of these numbers, in particular those of the natural numbers. Algebraically the elements of the set Z will be denoted by the symbols such as $a, b, c, \cdots, x, y, z$ etc. The methods and properties of *addition, subtraction and multiplication* are employed in the usual manner, but that *ofdivision* is of special attenti0n in the theory. The properties of the *prime numbers* defined in section 3, dealt comprehensibly in Number Theory, plays a central role in Cryptography. Their properties are presented here keeping in view the Cryptographic applications. The properties of difficulty of factorising large numbers, or taking their discrete logarithms, or selecting them from elliptic curves defined in section 11, are presented in a succint manner. These properties are central to the Cryptographic methods, and presented here in clear terms, using only elementary algebra.

DIVISIBILITY

Definition: Let a and b be integers. Then b is said to be divisible by $a \neq 0$ if $b = ax$, where x is an integer. In brief this definition is written as $a \mid b$ (meaning a divides b).

Examples. (i) $5 \mid 35$ since $35 = 5 \cdot 7$. (ii) $1 \mid 7$ since $7 = 1 \cdot 7$, (iii) $3 \mid -21$ since $-21 = 3 \cdot (-7)$.

Theorem 2.1

(i) If $a \mid b$ then $a \mid bc$.

(ii) If $a \mid b$ and $b \mid c$ then $a \mid c$.

(iii) If $a \mid b$ and $a \mid c$ then $a \mid (bx + cy)$ for integers x and y.

Proof. (i) and (ii) are self evident. For (iii) Let $b = ar$ and $c = as$ where r and s are integers. Therefore $bx + cy = a(rx + cy)$, that is $a \mid (bx + cy)$.

Theorem 2.2 (Division Algorithm). Given two integers a, b such that $a > 0$; then there exists unique inegers q, r such that

$$b = qa + r, \quad (0 \leq r < a) \tag{2.1}$$

Moreover if a does not divide b then $(0 < r < a)$.

Proof. Consider the sequence in Arithmetic Progression

$$\cdots\cdots, -4a, -3a, -2a, -a, 0, a, 2a, 3a, 4a, \cdots\cdots$$

Any integer b (positive, negative, or zero) is an element of the sequence or it lies between two conseqcutive elements. Thus, two numbers q and r can be determined uniquely so that $b = qa + r$, where $0 \leq r < a$. If a does not divide b, then $r \neq 0$.

Examples. (i) Let $a = 7, b = 22$, then $22 = 7 \cdot 3 + 1$. (ii) Let $a = 2, b = -53$, then $-53 = (-27) \cdot 2 + 1$.

GREATEST COMMON DIVISOR

Let $a \mid b$ and $a \mid c$. then a is a common divisor of b and c. Since there is only a finite number of divisors of any nonzero integer, there can only be a finite number of common divisors of b and c. The greatest among the divisors is called the *Greatest Common Divisors* denoted as $gcd(b, c)$. gcd is also known as *Greatest Common Measure (GCM)*, or as *Highest Common Factor (HCF)*. Evidently, $gcd(b, a) = gcd(a, b)$.

Lemma. Let a, b, c be integers then

$$gcd(a + cb, b) = gcd(a, b) \tag{2.2}$$

Proof. Actually all of the common divisors of $a + cb$ and b are exactly the same as those of a and b. For, let e be a common divisor of $a + cb$ and b, then $e|(a + cb)$ and e | b. Now by Theorem 2.1 (iii) it means that $e \mid [(a + cb) - cb]$ or $e \mid a$, that is e is a common divisor of a as well as that of b. Hence for the greatest divisor $gcd(a + cb, b) = gcd(a, b)$.

Theorem 2.3 (Euclidean Algorithm). Given integers b and $c > 0$, then by repeated application of the Division Algorithm,

$$\begin{array}{ll} b = cq_1 + r_1, & 0 \le r_1 < c \\ c = r_1q_2 + r_2, & 0 \le r_2 < r_1 \\ r_1 = r_2q_3 + r_3, & 0 \le r_3 < r_2 \\ \cdots\cdots\cdots\cdots & \cdots\cdots\cdots \\ r_{n-2} = r_{n-1}q_n + r_n, & 0 \le r_n < r_{n-1} \\ r_{n-1} = r_nq_n + 1 & \end{array} \qquad (2.3)$$

in which $c > r_1 > r_2 > r_3 > \cdots r_n > 0$. Since the number of remainders $< c$ is limted, a stage $n + 1$ will come when $r_n + 1 = 0$ and $gcd(b, c) = r_n$.

Proof. From the result of the Lemma given above

$$\gcd(b, c) = \gcd(c, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = r_n$$

The theorem was also stated independently by Aryabhat in verse form as was the custom in Sanskrit literature. This algorithm is particularly useful for calculating the *gcd* of large integers.

Example. Find $gcd(374, 1024)$.

By division using a calculator

$$\begin{aligned} 1024 &= 2 \cdot 374 + 276 \\ 374 &= 1 \cdot 276 + 98 \\ 276 &= 2 \cdot 98 + 80 \\ 98 &= 1 \cdot 80 + 18 \\ 80 &= 4 \cdot 18 + 8 \\ 18 &= 2 \cdot 8 + 2 \\ 8 &= 4 \cdot 2 + 0 \end{aligned}$$

Hence $gcd(374, 1024) = 2$.

The following theorem is also useful.

Theorem 2.4 (Extended Euclidean Theorem). If the numbers b and c are not both zero and $g = gcd(b, c)$, the there exist integers x_0, y_0 such that

$$g = bx_0 + cy_0 \qquad (2.4)$$

Proof. Consider the linear combination $bx + cy$, then it is negative, zero (when $x = 0, y = 0$) or positive. Let d be the least positive value of $bx + cy$ for $x = x_0$ and $y = y_0$; then $d = bx_0 + cy_0$. Let $b \neq 0$, then it follows that $d \mid b$ and $d \mid c$. For, by division algorithm

$$b = dq + r, \quad 0 \le r < d$$

or $$r = b - dq = b - (bx_0 + cy_0)\, q = (1 - qx_0)\, b = qy_0c$$

which is a linear combination of b and c. Since $0 \le r < d$ and d is the least positive combination of b and c, it follows that $r = 0$, and so $d \mid b$. In a similar manner $d \mid c$.

In order to show that $d = gcd(b, c)$, consider a number e such that $e \mid b$ and $e \mid v$. Hence according to Theorem 2.1 (iii), $e \mid (bx_0 + cy_0)$, that is $e \mid d$, so that $d \ge e$. Hence $g = gcd(b, c)$.

PRIME NUMBERS

Prime numbers are also known as Primes.

Definition: A *positive integer* which has no divisors except itself and 1 is called a *Prime Number*. Numbers which are not prime are called *Composite Numbers*.

Thus, for example, 2, 3, 5, and 7 are prime numbers where as 4, 6, 8, and 9 are composite numbers.

Definition: Two integers a and b are called prime to each other or coprime if $gcd(a, b) = 1$.

Theorem 3.1 A prime number p is prime to every number which is not a multiple of p.

Proof. Let a be a number which is not a multiple of p. Hence if a is divided by p, then according to the division algorithm $a = qp + r$, where $0 < r < p$. Now p and 1 are the only divisors of p, and as $r < p$, the only common divisors of p and r is 1, that is, $gcd(p, r) = 1$ or by Lemma of section 2.1, $gcd(a, p) = 1$, that is, a and p are prime to each other.

Theorem 3.2 Every composite number n has at least one prime divisor.

Proof. Since n is a composite number and not a prime, it has a divisor $1 < m < n$, which is not greater than any other divisor. Then m must be a prime; for otherwise it would have a divisor less than itself and greater than 1. The latter divisor would be a divisor of n. This contradicts the hypothesis that n is not greater than any other divisor.

Theorem 3.3 Every composite integer n greater than 1 can be expressed as a product of primes.

Proof. Since n has at least one prime factor p_1, $n = p_1 \cdot a$, where $1 < a < n$. If a is not a prime, it has at least one prime factor p_2 such that $a = p_2 \cdot b$, where $1 < b < a$. Thus $n = p_1 \cdot a = p_1 \cdot p_2 \cdot b$, and so on. But the numbers less than n are limited and $n > a > b > \cdots\cdots$ Therefore the set $\{n, a, b, \cdots\}$ must finally end in a prime. Hence n can be expressed as $n = p_1 \cdot p_2 \cdot p_3 \cdots p_l$, where $p_1, p_2, p_3, \cdots p_l$ are all primes not necessarily all different.

Thus, in general, a composite number n can be written as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots\cdots p_m^{\alpha_m} \qquad (3.1)$$

Theorem 3.4 (Fundamental Theorem of Arithmetic) The factorisation of a composite number n is unique.

Proof. Let n have two different factorings:

$$p_1 \cdot p_2 \cdot p_3 \cdots\cdots p_r = q_1 \cdot q_2 \cdot q_3 \cdots\cdot q_s$$

where p_i, q_j are primes not necessarily distinct, but no prime on the left-hand side occurs on the right side. This means that $p_1 \mid q_1 \cdot q_2 \cdots\cdots q_s$, that is, p_1 is a divisor of at least one of the q_j, which means that p_1 equals at least one of the q_j, contradicting the hypothesis.

Theorem 3.5 There are infinitely many primes.

Proof. Let p be the largest prime. Then the number $p! + 1$ is greater than p and is not divisible by p or any smaller value of p. If $p! + 1$ is not a prime, it must have a prime factor greater than p. Hence, in either case, a prime number greater than p exists.

Theorem 3.6 If n is a composite integer, then n has a prime factor less than or equal to $\sqrt{n}$.

Proof. Let $n = a \cdot b$, where a is a prime and $b \geq a$, then $n \geq a_2$, so that $a \leq \sqrt{n}$.

Example 1. Find all the primes less than 20.

Here $n = 20$ and $\sqrt{n} = \sqrt{20} = 4.4721$. Now the only primes less than or equal to 4.4721 are 2 and 3. Hence, rejecting all the whole numbers up 20 that are divisible by 2 and 3 yield the prime numbers

2, 3, 5, 7, 11, 13, 17, and 19.

Example 2. Find all the primes less than 100.

Here $n = 100$, and $\sqrt{n} = \sqrt{100} = 10$. The primes less than 10 are 2, 3, 5 and 7. Hence checking allthe integers up to 100 for divisibility by 2, 3, 5, 7 and rejecting the divisible ones yield the primes

2, 3, 5, 7, 11, 13, 17, 19
23, 29, 31, 37, 41, 43, 47, 53
59, 61, 67, 71, 73, 79, 83, 89, 97

Examples 1 and 2 illustrate the *Seive of Eratosthenes* for generating prime numbers.

The prime numbers appear to be distributed randomly. Estimation of their distribution was a major problem which was finally resolved by Chebyshev as stated below.

Theorem 3.7 (Prime Number Theorem). Let $\pi(x)$ denote the number of primes less than or equal to a real number x, then

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1 \qquad (3.2)$$

or, $$\pi(x) \sim \frac{x}{\log x} \text{ as } x \to \infty$$

The proof of this theorem is very technical and outside the scope of this article.

CONGRUENCE

Definition: Let m be any positive integer, called *modulus.* If a and b are any two integers positive or negative such that $m|\ (a - b)$, then a and b are said to be congruent with respect to modulus m, and each of a and b is said to be the residue of the other. This is expressed by writing

$$a \equiv b \pmod m \text{ or } a - b \equiv 0 \pmod m \qquad (4.1)$$

where ≡ stands for "congruent with".

Theorem 4.1 $a \equiv b \pmod m$ if and only if there is an integer k such that $a = b + km$.

Proof. If $a \equiv b \pmod m, m|\ (a - b)$ and therefore there exists an integer k, such that $(a - b)/m = k$ or $a = b + km$. Conversely if $a = b + km$ then, $(a - b)/m = k$ and so $a \equiv b \pmod m$.

Thus, letting k to have the values $\cdots\cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4.\cdots\cdots$ one gets the arithmetic progression

$$\cdots\cdots, b - 4m, b - 3m, b - 2m, b - m, b, b + m, b + 2m, b + 3m, b + 4m, \cdots\cdots$$

called the *residue class* modulo m, or alternatively the congruence class modulo m.

Example 1. Let $m = 12$ (as with a clock), then $8 \equiv 8 \pmod{12}$ and $17 \equiv 5 \pmod{12}$. For, $(8 - 8)/12 = 0/12 = 0$, and $(17 - 5)/12 = 12/12 = 1$. Hence $12 \mid (8 - 8)$ and $12 \mid (17 - 5)$ from which the two results follow.

Example 2. Let $m = 26$ (as with the 26 letters A, B, C, D, $\cdots\cdots$, X, Y, Z), then $13 \equiv 13 \pmod{26}$, and $29 \equiv 3 \pmod{26}$.

Theorem 4.2 If r is the remainder when a is divided by m, then

$$a \equiv r \pmod m \text{ and } 0 \le r < m \qquad (4.2)$$

Proof. By the division algorithm Eq. (2.2) if q is the quotient when a is divided by $m, a = qm + r$ where $0 \le r < m$. Hence, $m|\ (a - r)$ so that $a \equiv r \pmod m$ with $0 \le r < m$. The expression in (3.2) is then an alternative way of expressing the division algorithm. Evidently, r is a member of the set $\{0, 1, 2, 3, \cdots\cdots, m - 1\}$ to which a is congruent. In this sense this set of elements is called the *complete set of residues* modulo m.

Theorem 4.3 Let $a \equiv b \pmod m$ and $a' \equiv b' \pmod m$, then

$(i) a + a' \equiv b + b' \pmod m$

$(ii)\ a - a' \equiv b - b' \pmod m$

$(iii) aa'(mod\ m) \equiv bb' \pmod m$

(iv) If a and b are divisible by d which is prime to m, then $a/d \equiv b/d \pmod m$

Proof. By hypothesis $m|\ (a - b)$ and $m|\ (a' - b')$. Thus,

$$m|\ [(a - b) \pm (a' - b')] \text{ or, } m|\ [(a \pm a') - (b \pm b')]$$

which proves (i) and (ii). For (iii)

$$aa' - bb' = (a - b)\,a' + (a' - b')\,b$$

in which $m|\,(a - b)$ and $m|\,(a' - b')$ and so $m|\,(aa' - bb')$. For (iv), $m|\,(a - b)$, so that $a - b = qm$ where q is an integer. By hypothesis, $d \mid (a - b)$, that is $d \mid qm$. But d and m are prime to each other, hence $d \mid q$, which means that q/d is an integer. Now, $a/d - b/d = (q/d) \cdot m$ and therefore $a/d \equiv b/d \pmod{m}$.

Remark. In particular, if $a \equiv b \pmod{p}$ where p is a prime and d is any common divisor of a and b, then $a/d \equiv b/d \pmod{p}$ except when $d \equiv 0 \pmod{p}$. Thus, there is a close analogy between congruence to a prime modulus and equalities.

To summarise, in dealing with integers modulo m, we are essentially performing the operations of arithmetic, but are disregarding multiples of m.

Theorem 4.4 If p is a prime number and a, b are any integers, then

$$(a + b)^p \equiv a^p + b^p \pmod{p} \qquad (4.3)$$

Proof. By the binomial theorem

$$(a + b)^p = \sum_{r=0}^{p} \binom{b}{r} a^{p-r}\, b^r$$

$$= a^p + b^p + \sum_{r}^{p} \binom{p}{r} a^{p-r}\, b^r$$

or, $$(a + b)^p - (a^p + b^p) = \sum_{r=1}^{p-1} \frac{p(p-1)(p-2)\cdots(p-r+1)}{r!} a^{p-r} b^r$$

The binomial coefficient on the right-hand side isa multiple of p which can not be divided by $r!$. This means that the product $(p - 1)(p - 2) \cdots (p - r + 1)$ is divisible by $r!$ as the binomial coefficients are all integers. Hence the congruence (4.3) from the above equation.

Remark. The above theorem can be easily generalised to any number of terms $a, b, c, \cdots, l$ as

$$(a + b + \cdots + l)^p \equiv a^p + b^p + \cdots + l^p \pmod{p} \qquad (4.4)$$

by successively increasing the number of terms to $3, 4, \cdots, l$.

From the above theorem follows one of the most basic theorem of number theory'

Theorem 4.5 (Fermat's Little Theorem) If p is prime and a is an integer prime to p, then

$$a^p - 1 \equiv 1 \pmod{p} \qquad (4.5)$$

Proof. Partitioning a in to $1s$, let $a = 1 + 1 + \cdots + 1$ (a terms), then by Eq. (4.4)

$$(1 + 1 + 1 + \cdots + 1)^p \equiv 1^p + 1^p + \cdots 1^p \pmod{p}$$

where there are a terms in the sums on both sides of the cogruence. Hence,

$$a^p \equiv a \pmod{p} \qquad (4.6)$$

Dividing by a and applying Theorem 4.3 (iv), we obtain (4.5).

Remark. The theorem can also be stated as the congruence (4.6).

Theorem 4.6 If p is prime and a is prime to p, then

$$a^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod{p}$$

Proof. $a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$ is divisible by p according to congruance (4.5). Therefore $p \mid \left(a^{\frac{p-1}{2}} - 1\right)$ or, $p \mid \left(a^{\frac{p-1}{2}} + 1\right)$. Hence,

$$\left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \pmod{p} \text{ or } \left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}$$

that is, $\left(a^{\frac{p-1}{2}} \pm 1\right) \equiv 0 \pmod{p}$, which establishes the theorem.

EULER'S PHI FUNCTION

Euler generalised Fermat's little theorem for any integer a, which may be a composite number

Definition. Let n be a positive integer. Euler's phi function $\phi(n), n > 1$ is defined as the number of integers less than n that are prime to n, with the stipulation that 1 is regarded as prime which is prime to every number such that $\phi(1) = 1$. Thus,

$$\phi(2) = 1\ (1)$$
$$\phi(3) = 2\ (1, 2)$$
$$\phi(4) = 2\ (1, 3)$$
$$\phi(5) = 4\ (1, 2, 3, 4)$$
$$\phi(6) = 2\ (1, 5)$$
$$\phi(7) = 6\ (1, 2, 3, 4, 5, 6)$$
$$\phi(8) = 4\ (1, 3, 5, 7)$$
$$\phi(9) = 6\ (1, 2, 4, 5, 7, 8)$$
$$\phi(10) = 4\ (1, 3, 7, 9), \text{ etc.}$$

Theorem 5.1 If a is prime to n, the number of terms of the arithmetic progression

$$x, x + a, x + 2a, \cdots\cdots, x + (n - 1)a$$

that are prime to n is $\phi(n)$.

Proof. Let these numbers be divided by n, then the remainders are $0, 1, 2, \cdots, n - 1$ (Theorem 4.2), taken in a certain order. Now, if a number is prime to n, so also its remainder. Consequently, as many terms in the progression are prime to n as there are numbers less than n and prime to it, that is $\phi(n)$.

Theorem 5.2 If m is prime to n, then

$$\phi(mn) = \phi(m) \cdot \phi(n) \text{ (multiplication property)} \qquad (5.1)$$

Proof. Let the numbers $1, 2, 3, \cdots, mn$ be arranged in an array of m columns and n rows as follows:

$$\begin{array}{ccccccc} 1 & 2 & \cdots & k & \cdots & m \\ m+1 & m+2 & \cdots & m+k & \cdots & 2m \\ 2m+1 & 2m+2 & \cdots & 2m+k & \cdots & 3m \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+k & \cdots & nm \end{array}$$

Since m is prime to n, the numbers prime to mn are prime to both m and n. Consider the k^{th} column. If for this column k is prime to m, then the elements of the column headed by k are prime to m and hence are members of $\phi(m)$. It follows that in the contrary case of k not prime to m, that column must be ignored. Now the elements of a desired column are $k, k + m, k + 2m, \cdots, k + (n - 1)m$ in which m is prime to n, These elements being in arithmetic progression, the number of terms prime to n is $\phi(n)$. Hence the total count of elements prime to mn is $\phi(m) \cdot \phi(n)$, that is $\phi(mn) = \phi(m) \cdot \phi(n)$.

Remark. The theorem can evidently be extended to any number of terms $m_1, m_2, \cdots, m_l$.

Theorem 5.3 (Euler's Theorem) If a is any number prime to n, then

$$a^{\phi(n)} \equiv 1 \pmod{n} \qquad (5.2)$$

Proof. Let $a_1(= 1), a_2, a_3, \cdots, a_{\phi(n)}$ be the numbers in ascending order less than n and prime to it. Consider the products

$$aa_1, aa_2, aa_3, \cdots, aa_{\phi(n)}$$

If these products are divided by n, the remainders are all different. For, if aa_r and aa_s $(r < s)$ give the same remainder, then $a(a_s - a_r)$ would be divisible by n. This is impossible since a is prime to n and $a_s - a_r < n$. Also, the remainders are all prime to n, for the factors a and a_r are all prime to n. Hence, by the product theorem 4.3 (iii),

$$(aa_1) \cdot (aa_2) \cdot \cdots \cdot \left(aa_{\phi(n)}\right) \equiv a_1 \cdot a_2 \cdot \cdots \cdot a_{\phi(n)} \pmod{n}$$

Dividing by $a_1 a_2 \cdots a_{\phi(n)}$ which is prime to n, $a^{\phi(n)} \equiv 1 \pmod{n}$.

Remark. Let p be a prime and a be a number prime to p, then the arithmetic progression $a, 2a, 3a, \cdots, (p-1)a$ are all prime to p. For this arithmetic progression $\phi(p) = p - 1$ and so $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's theorem.

Theorem 5.4 If p is prime, then

$$\phi(p^r) = p^r(1 - 1/p) \qquad (5.3)$$

Proof. When $r = 1$, the numbers $1, 2, 3, \cdots (p-1)$ are all prime to p. Hence $\phi(p) = p - 1 = p(1 - 1/p)$. When $r > 1$, since p is prime; of the numbers $1, 2, 3, \cdots, p^r$ those which are not prime to p^r are $p, 2p, 3p, \cdots p \cdot p^{r-1}$ which are p^{r-1} in number. all the rest are prime to p^r and their number is $p^r - p^{r-1} = p^r(1 - 1/p)$.

Theorem 5.5 If any number $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_l^{\alpha_l}$ are the prime factors of n, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \ldots \ldots \left(1 - \frac{1}{p_l}\right)$$

Proof. $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots \ldots, p_l^{\alpha_l}$ are prime to one another and so the theorem follows from Theorem 5.4 and the Remark after 5.2.

Theorem 5.6 (Wilson's Theorem) If p is a prime number, then

$$(p-1)! \equiv -1 \pmod{p} \qquad (5.5)$$

Proof. Let a be any one of the numbers $1, 2, 3, \cdots, p-1$. If the products $1a, 2a, 3a, \cdots, (p-1)a$ are divided by p, the remainders are $1, 2, 3, \cdots, p-1$ (by theorem 4,2) in a certain order. Hence for every a there is a unique number a' such that $a'a$ is divided by p leaves the remainder 1, that is, $aa' \equiv 1 \pmod{p}$. If now $a' = a$, then $aa' - 1 = a'^2 - 1$ must be divisible by p, which means that $a-1$ or $a+1$ is divisible by the prime p. Since $a < p$, it follows that either $a' = a = 1$ or $p-1$. If then, $a' = 2, 3, \cdots p-2$ it can not be equal to a. Now, these $p = 3$ even numbers can be arranged in $\frac{1}{2}(p-3)$ pairs, such that the product of each is congruent to 1 modulo p. Hence,

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$$

or

$$(p-1)! \equiv p-1 \pmod{p} \equiv -1 \pmod{p}$$

which proves the result (5.5).

Remark. The theorem is true only when p is prime. For otherwise assume that p has a factor q, which must be less than p and therefore must divide $(p-1)!$. Hence $(p-1)! + 1$ is not a multiple of q and therefore not a multiple of p.

FAST EXPONENTIATION

In Cryptography the raising of power of a number (or exponentiation) as in Fermat's and Euler's theorem for large values of the power is common place. In such cases straight forward calculation even with the aid of a computer becomes prohibitive. To overcome this difficulty, a Fast Exponentiation algorithm has been developed, which is described below.

Suppose one has to calculate $a^n \pmod{n}$ where n is large. Expressing the exponent n in binary digits to the base 2, one can express n as a polynomial in this base number as

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 2^2 + \cdots\cdots + n_l \cdot 2^l \qquad (6.1)$$

where $n_0, n_1, n_2, \cdots, n_l \in \{0, 1\}$ with $n_l = 1$. As for example, let $n = 563$, then one can write

$$563 = 1 + 2 + 24 + 25 + 29 = 1100110001 \quad \text{(binary)}$$

Thus, a^n can be written as

$$a^n = a^{(n_0 + 2n_1 + 2^2 n_1 + \cdots 2^l n_l)}$$
$$= a^{n_0} \cdot (a^2)^{n_1} \cdot \left(a^{2^2}\right)^{n_2} \cdots\cdots\cdots\cdots \left(a^{2^l}\right)^{n_l}$$

Now the sequence $a, a^2, a^{2^2}, \cdots \ldots, a^{2^l}$ can be easily computed *modulo* n by recursion. Let

$$b_0 := a \pmod{n}$$
$$b_1 := b_0^2 \equiv a^2 \pmod{n}$$
$$b_2 := b_1^2 \equiv a^{2^2} \pmod{n}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$b_l := b_{l-1}^2 \equiv a^{2^l} \pmod{n}$$

which yields

$$a^n \equiv b_0^{n_0} \cdot b_1^{n_1} \cdot b_2^{n_2} \cdots\cdots b_l^{n_l} \pmod{n} \qquad (6.2)$$

in which the product on the right-hand side of (6.2) can be computed by at most l multiplications, as any exponent $n_k = 0$ will contribute only 1 as a factor.

LINEAR CONGRUENCE

Definition: A congruence of the form

$$ax \equiv b \pmod{m} \qquad (7.1)$$

where x is an unknown integer is called a *linear congruence* in one variable.

In a linear congruence, it is to be noted that if $x = x_0$ is a solution of (7.1), and if $x_1 \equiv x_0 \pmod{m}$, then $ax_1 \equiv ax_0 \equiv \pmod{m}$ so that x_1 is also a solution of (7.1). Hence if one member of a congruence class modulo m is a solution, then all members of this class are also solutions. Hence, one may seek *incongruent solutions* modulo m of (7.1).

Theorem 7.1 If a and m be relatively prime integers with $m > 0$ and b an integer, then the linear congruence $ax \equiv \pmod{m}$ has a *unique solution* $x_0 < m$ modulo m.

Proof. With modulo m the integers are the terms of the arithmetic progression $0, a, 2a, \cdots\cdots, (m-1)a$. If divided by m, since a is prime to m, the remainders are $0, 1, 2, \cdots\cdots, (m-1)$ in a certain order, and by the division algorithm (theorem 4.2) , the latter set is also the set when b is divided by m. Hence, there exists just one x_0 such that $ax_0 \equiv b \pmod{m}$, where $0 \leq x_0 < m$.

Theorem 7.2 Let a be not prime to $m > 0$, such that $gcd(a, m) = g > 1$, and b an integer. If g does not divide b, then $ax \equiv b \ (mod\ m)$ has no solution. If g divides b then the equation has exactly g *incongruent solutions* modulo m.

Proof. Let $a = ga'$ and $m = gm'$ so that a' is prime to m'. We require that $ga'x - b$ is divisible by gm'. Hence, if g does not divide b, there is no solution. Next suppose that g divides b, that is $b = gb'$, then $a'x - b'$ is divisible by m' if $a'x \equiv b' \pmod{m'}$. Since a' is prime to m', the last congruence has exactly one solution $x_0 < m'$ and g incongruent solutions $x_0, x_0 + m', x_0 + 2m', \cdots\cdots, x_0 + (g-1)m'$ which are distinct roots of $ax \equiv b \pmod{m}$.

Theorem 7.3 (Simultaneous Congruences: Chinese Remainder Theorem) Let m_2 be prime to m_1, then the solution of the simultaneous congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2} \tag{7.2}$$

is given by the solution of $x \equiv x_1 \pmod{m}$, where $m = m_1 m_2$.

Proof. From the first congruence relation of (7.2), one gets $x = a_1 + m_1 y$. Substituting in the second congruence relation, one has $m_1 y \equiv a_2 - a_1 \pmod{m_2}$. Since m_1 and m_2 are relatively prime, this congruence has a unique solution y_1 modulo m_2, so that $y = y_1 + lm_2$. Thus, the general solution is

$$x = a_1 + m_1(y_1 + m_2 l) = x_1 + ml$$

where $x_1 = a_1 + m_1 y$, and $m = m_1 m_2$. Hence the theorem.

Remark. The theorem can be generalised to three, four. $\cdots\cdots$ congruences in steps and in general to n congruences as follows. Let,

$$x \equiv a_1 \pmod{m_1}, \ x \equiv a_2 \pmod{m_2}, \cdots\cdots, x \equiv a_n \pmod{m_n} \tag{7.3}$$

where $m_1, m_2 \cdots\cdots, m_n$ are mutually prime to each other, the solution of (7.3) is the same as that of $x \equiv x_m \pmod{m}$ where $m = m_1 m_2 \cdots\cdots m_n$.

PRIMALITY TESTING

In Cryptography testing a given number n, often very large, is of paramount importance. We proceed to study some of the testing methods with their merits and demerits.

TRIAL DIVISION

According to theorem 3.6, if n is a composite number, then it has a prime divisor $p \leq \sqrt{n}$. If no such prime divisors are found then n is a prime number.

Example. Test $n = 561$ and 563 for primality.

In the first case using a calculator $\sqrt{n} = 23.68543\ldots$.. and in the second case $\sqrt{n} = 23.72762\ldots$.., which means that the integral part $\lfloor \sqrt{n} \rfloor = 23$. Now the prime numbers less than or equal to 23 are $2, 3, 5, 7, 11, 13, 17, 19$ and 23. From this set $3 \mid 561$ and therefore 561 is a composite number. But none from the set divides 563 and so 563 is a prime number.

Remark. In the RSA cryptosystems employed in practice, primes greater than 10^{75} are required, that entails following the prime number theorem at least 10^{35} divisions for the test, which is an impossible task.

FERMAT TEST

According to Fermat's little theorem (Theorem 4.5), if for an integer a prime to n can be found, such that

$$a^{n-1} \equiv 1 \pmod{n} \qquad (8.1)$$

then n is *likely* a prime number. The statement "likely" is emphasised because the converse of the theorem is not always true. The smallest number which shows the inadequacy of the Fermat test is $n = 341 - 11 \cdot 31$. For

$$\begin{aligned} 2^{341-1} = 2^{340} = (2^{10})^{34} = 1024^{34} = (1023 + 1)^{34} \\ = (3 \cdot 341 + 1)^{34} \equiv 1^{34} \pmod{341} \\ \equiv 1 \pmod{341} \end{aligned}$$

Worst is the case of $n = 561 = 3 \cdot 11 \cdot 17$, with *arbitrary* a prime to n, showing that $a^{n-1} = a^{560} \equiv 1 \pmod{561}$. This is proved in three steps.

First Step; Modulo 3: If a is prime to 3, then by Fermat's littele theorem

$$a^2 \equiv 1 \pmod{3}; \text{ and so } a^{560} \equiv (a^2)^{280} \equiv 1^{280} = 1 \pmod{3}$$

Second Step; Modulo 11: If a is prime to 11, then similarly

$$a^{560} = (a^{10})^{56} = (a^{11-1})^{56} \equiv 1^{56} = 1 \pmod{11}$$

Third Step; Modulo 17: If a is prime to 17, then

$$a^{560} = (a^{16})^{35} = (a^{17-1})^{35} \equiv 1^{35} = 1 \pmod{17}$$

Hence by the Chinese remainder theorem 7.3 for all a satisfying $gcd(a, 561) = 1$

$$a^{560} = a^{561-1} \equiv 1 \pmod{3 \cdot 11 \cdot 17 = 561}$$

Numbers such as $n = 561$ are called Carmichael Numbers. Such special numbers are rare. For instance, there are only 1,00,000 Carmichael numbers less than 10^{15}.

Theorem 8.1 If $n = p_1 \cdot p_2 \cdot \cdots \cdot p_l$ is a product of *distinct* primes, such that $(p_i - 1) \mid (n - 1)$ for all i, then n is a Carmichael number.

Proof. Let a be an integer prime to n and p_i a prime divisor of n. Then, $a^{p_i-1} \equiv 1 \pmod{p_i}$. Therefore, $a^{n-1} \equiv 1 \pmod{p_i}$ as $n - 1$ is a multiple of $p_i - 1$. Hence by the Chinese remainder theorem, $a^{n-1} \equiv 1 \pmod{p_1 \cdot p_2 \cdot \cdots \cdot p_l = n}$.

MILLER-RABIN TEST

Here Fermat's theorem is so modified as to exclude the possibility of Carmichael numbers.

Theorem 8.2 Let p be prime such that $p - 1 = 2^k q$ where q is odd. Let a be any number prime to p, then either $(i) a^q \equiv 1 \pmod{p}$, or

$$(ii) \text{ One of } a^q, a^{2q}, \cdots\cdots, a^{2^{k-1}q}, a^{2^k q} \equiv -1 \pmod{p}.$$

Proof. By Fermat's theorem, $a^{p-1} \equiv 1 \pmod{p}$, in which $p - 1 = 2^k q$. Consider therefore the sequence

$$a^q, a^{2q}, \cdots\cdots, a^{2^{k-1}q}, a^{2^k q}$$

which form elements of a sequence of the previous powers. Hence

(i) For the first element $a^q \equiv 1 \pmod{p}$, or

(ii) Some number in the list is not congruent to *1* modulo p. But when it is squared, it becomes congruent to 1 modulo p. But the only number satisfying both $b \not\equiv 1 \pmod{p}$ and $b^2 \equiv 1 \pmod{p}$ is $b \equiv -1 \pmod{p}$. So one of the numbers in the list is -1 module p. This proves the theorem.

This test is often used in practice.

Example. Show that 561 is composite.

The number 2 is prime to p, so let $a = 2$. Therefore $q = 560/2^k = 35$ (odd) for $k = 4$, using a calculator. Therefore

$$2^{35} \equiv 2^{63} \pmod{561}$$
$$2^{35 \cdot 2} \equiv 263^2 \pmod{561} \equiv 166 \pmod{561}$$
$$2^{35 \cdot 4} \equiv 166^2 \pmod{561} \equiv 67 \pmod{561}$$
$$2^{35 \cdot 8} \equiv 67^2 \pmod{561} \equiv 1 \pmod{561}$$

None of the above values equal -1 and so 561 is composite.

AKS TEST

The Agrawal, Kayal, Saxena test was discovered in recent years (2022). It is based on Theorem 3.4 in the form that if x is any integer and a is prime to the prime number n, that is to say $gcd(a, n) = 1$, then

$$(x + a)^n \equiv x^n + a^n \equiv x^n + a \pmod{n}$$

by Fermat's little theorem (4.6). It was shown that the modulus n can be further reduced to

$$(x + a)^n \equiv x^n + a \pmod{(x^r - 1 \bmod n)}$$

when $a < n$, showing that when a is below a certain limit, then n is a prime. The method consists of the following procedure:

1) Find the smallest power k such that $n^k \equiv 1 \pmod{r}$.
2) Find the smallest r such that $k > (log\ n)^2$
3) If $1 < gcd(a, n) < r$ for some $a \leq r$, then x is *COMPOSITE*
4) If $n \leq r$, then x is *PRIME*; stop.
5) For a from 1 to $\lfloor \sqrt{\phi(r)}\ \log n \rfloor$ do:
   if $(x + a)^n \not\equiv x^n + a \pmod{(x^r - 1 \pmod{n})}$
   then x is *COMPOSITE*; stop. Otherwise
6) x is PRIME

The Proof of this method is given in Dietzfellinger (2004). Although the method appears quite intricate, it has been shown that its algorithm has a polynomial complexity.

FACTORISING

Given a composite number $n = pq$, it is required to find the prime factors p and q of n,

POALLARD'S P-1 METHOD

Since p is prime, $p - 1$ is an even number. *Assume* that $p - 1$ has only small prime factors, and let k be a *multiple* of $p - 1$, that is, $k = (p - 1)\ i$. Hence,

$$a^k = a^{(p-1)i} = (a^{p-1})^i \equiv 1 \pmod{p} \tag{9.1}$$

by Fermat's theorem, in which a is randomly chosen. The above congruence means that $p \mid (a^k - 1)$. As $p \mid n$, it then means that

$$p = gcd(a^k - 1, n) \tag{9.2}$$

in which k is a multiple of $p - 1$ and is even.

In practice a is usually chosen as 2. If the gcd equals n, then a different a is chosen. The value of k is taken as $k = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots\cdots p_l^{\alpha_l}$, where $p_1, p_2, p_3 \cdots\cdots, p_l$ are primes. It transpires that the selection of (p_i, α_i) is practically possible when k and p_i have small values, and so if n and k are large, the factorisation is very hard. Once the value of p is found, q is obtained as $q = n/p$.

Example. Factorise $n = 1105$ (the second Carmichael number).

Choose $a = 2$.

If $k = 2$, $a^k - 1 = 2^2 - 1 \equiv 3$, and $gcd(3, 1105) = 1$.

If $k = 2^2, a^k - 1 = 2^4 - 1 \equiv 15$, and $gcd(15, 1105) = 5$.

Hence $p = 5$. Therefore $q = 1105/5 = 221$.

If $k = 2^2, a^k - 1 = 2^4 - 1 \equiv 15$, and $gcd(15, 221) = 1$.

If $k = 2^3, a^k - 1 = 28 - 1 \equiv 255$, and $gcd(255, 221) = 17$.

Hence, $q = 17$, and therefore $r = 221/17 = 13$. Thus, $n = 5 \cdot 13 \cdot 17$.

POLLARD'S RHO METHOD

Let $n = pq$ as before. The Rho method is based on generating a suitably large sequence of pseudo-random numbers by congruence modulo n. Let the sequence be generated iteratively according to the iteration

$$x_i \equiv f(x_{i-1}) \pmod{n}\ i = 1, 2, 3, \cdots\cdots \tag{9.3}$$

with seed $x_0 = 2$, and f a nonlinear function. It has been found empirically that

$$\mathrm{f}(x) = x_2 + 1 \tag{9.4}$$

generates the required type of sequence from (9.3).

This sequence is cyclic composed of n distinct elements. Now, if d be an integer such that

$$x_i \not\equiv x_j \pmod{n} \tag{9.5}$$

and

$$x_i \equiv x_j \pmod{d} \tag{9.6}$$

then the sequence is also cyclic modulo d; because

$$x_{i+1} \equiv f(x_i) \equiv f(x_j) = x_{j+1} \pmod{d} \tag{9.7}$$

The length of the sub-cycle is $d = J - i$. To illustrate this point, consider the case of $n = 323 = 17 \cdot 19$, then the sequence according to (9.3) is

$$2, 5, 26, \underline{31, 316, 50, 24o, 107, 145,}\ \underline{31, 316, 50, 24o, 107, 145,} \cdots\cdots$$

in which the sub-cycle is underlined for identification.

In order to detect the sub-cycle modulo p, consider the sequence

$$\begin{aligned} y_0 &= x_0 \\ y_k &= x_{2k},\ k = 1, 2, 3, \cdots\cdots \end{aligned} \tag{9.8}$$

The cycle for p is given by

$$p = gcd(|y_k = x_k|, n) \neq 1 \tag{9.9}$$

Alternatively, one may consider the iteration generated by the sequence $\{x_i\}$ according to

$$\begin{aligned} y_0 &= x_0 \\ y_k &= f\big(f(y_{k-1})\big),\ k = 1, 2, 3, \cdots\cdots \end{aligned} \tag{9.10}$$

and consider the gcd (9.9) to yield the value of p.

The other factor q is given by $q = n/p$.

The method has been found to be of practical use when p is less than ten digits long.

DISCRETE LOGARITHM

Let a and b be two elements of a cyclic group of n elements $\{0, 1, 2, 3, \cdots\cdots, n-1\}$, which recur repeatedly in a chain. If x is the *smallest* nonnegative integer modulo n of the set such that

$$a^x = b \tag{10.1}$$

then x is called the *discrete logarithm* of b to the base a, written as $x = \log_a b \pmod n$. In cryptographic applications, the existence of x is typically guarenteed.

A very simple but expensive method of finding x is by enumeration, testing $x = 0, , 1, 2, \cdots\cdots, n-1$ to test whether a^x equals b. As soon as an x value is found the testing is stopped, yielding the value of the logarithm. However, better methods have been devised as presented below.

SHANK'S BABY STEP - GIANT STEP METHOD

In this method, the upper integer part of $\sqrt{n}$ is set as

$$m = \left[\sqrt{n}\right] + 1 \tag{10.2}$$

where $[\cdot]$ is the (lower) integer part of n. The unknown discrete logarithm x is then represented as

$$x = qm + r,\quad (0 \leq r < m) \tag{10.3}$$

by the division algorithm, in which q and r are respectively the quotient and the remainder when x is divided by m. Thus,

$$a^{qm+r} = a^x = b \tag{10.4}$$

or,
$$(a^m)^q = ba^{-r} \tag{10.5}$$

In the above Eq. (10.5), compute the set of *baby steps*:

$$B = \{(b\,a^{-r}, r), \quad 0 \leq r < m\} \tag{10.6}$$

Now, in the set B look for a pair $(1, r)$, then $ba^{-r} = 1$, or $a^r = b$, and thus $x = r$.

If in the set B the pair $(1, r)$ is not found, set $c = a^m$ and test for $q = 1, 2, 3, \cdots\cdots$ the remainder c^q. If this number is the first component of an element in B, that is, $(c^q, r) \in B$, then

$$ba^{-r} = c^q = a^{mq} \tag{10.7}$$

so that $b = a^{mq+r} = a^x$, and the discrete logarithm is $x = qm + r$. The steps $c^q, q = 1, 2, 3 \cdots\cdots$ are called *giant steps*.

Example. Find $\log_3 8 \pmod{17}$.

Here $n = 17, 3^x = 8 (\text{mod } 17), m = [\sqrt{17}] + 1 = 4 + 1 = 5, x = qm + r$ with $0 \leq r < 5$. We therefore form a table for B:

r	$8 \cdot 3^{-r} \pmod{17}$
0	8
1	2
2	8
3	8
4	8
5	8

None of the values in the second column equals 1. The baby steps do not yield the required logarithm. Hence set $c = 3^m = 3^5 = 243 \pmod{17} = 5$ for the giant step. Hence, we form the table

q	$c^q \pmod{17}$
1	5
2	$5^2 \equiv 8$

Therefore, the solution is $q = 2, r = 0$. Hence, $x = 2 \cdot 5 + 0 = 10$.

POHLIG - HELLMAN METHOD

In this method in order to find $x = \log_a b \,(\text{mod } n)$, where x is an element of the cyclic group of n elements $\{0, 1, 2, 3, \cdots\cdots, n - 1\}$ so that $a^n = a^0 = 1$, let n be factored in to primes (Theorem 3.3) as

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots\cdots p_l^{\alpha_l} \tag{10.8}$$

Also, for each prime divisor p_i of n, let

$$n_i = n/p_i^{\alpha_i}, \; a_i = a^{n_i}, \; b_i = b^{n_i} \tag{10.9}$$

then it follows that a_i is an element of a cyclic group of $p_i^{\alpha_i}$ elements, and so

$$x_i = \log_{a_i} b_i \pmod{p_i^{\alpha_i}} \tag{10.10}$$

exists,

Now consider the simultaneous congruences

$$x \equiv x_i \pmod{p_i^{\alpha_i}}\ i = 1, 2, 3, \cdots\cdots, l \tag{10.11}$$

whose solution by the Chinese Remainder Theorem is of modulus $\left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots\cdots p_l^{\alpha_l}\right)$ or (mod n). We assert that the solution of the system (10.11) is $x_c = \log_a b \pmod{n}$, since

$$x_c = x_i + p_i^{\alpha_i} y_i \text{ for some } y_i \tag{10.12}$$

Hence,

$$\begin{aligned}(a^{x_i})^{n_i} &= \left(a^{x_i + p_i^{\alpha_i} y_i}\right)^{n_i} \\ &= a^{x_i n_i + n y_i} = a_i^{x_i} \cdot a^{n y_i} \\ &= a_i^{x_i} \cdot (1)^{y_i} = a_i^{x_i} = b_i = b^{n_i}\end{aligned}$$

or,

$$\frac{n}{p_i^{\alpha_i}} x_i \equiv \frac{n}{p_i^{\alpha_i}} \log_a b \pmod{n} \tag{10.12}$$

Now, the number

$$\frac{n}{p_1^{\alpha_1}}, \frac{n}{p_2^{\alpha_2}}, \cdots\cdots, \frac{n}{p_l^{\alpha_l}}$$

have no common factor except 1, that is their $gcd = 1$. Hence by the extended Euclidean algorithm (Theorem 2.4), integers $c_1, c_2, \cdots\cdots, c_l$ exist such that

$$\frac{n}{p_1^{\alpha_1}} c_1 + \frac{n}{p_2^{\alpha_2}} c_2 + \cdots\cdots + \frac{n}{p_l^{\alpha_l}} c_l = 1 \tag{10.13}$$

Thus, multiplying both sides of (10.12) by c_l and sum over $i = 1, 2, \cdots\cdots, l$, one obtains

$$\sum_{i=1}^{l} \frac{n}{p_i^{\alpha_i}} c_i \cdot x_i \equiv Xl\ i = \sum_{i=1}^{l} \frac{n}{p_i^{\alpha_i}} c_i \cdot \log_a b \pmod{n} \tag{10.14}$$

or, $x_i = \log_a b \pmod{n}$. The problem therefore reduces to solution of the system of congruences (10.11), by say Shank's baby step giant step method.

Remark. In the above method, if $\alpha_i > 1$, it is possible to further reduce the modulus from $p_i^{\alpha_i}$ to p_i. As a generic form consider the solution of

$$a^x = b \pmod{p^\alpha} \tag{10.15}$$

to find $\log_a b \pmod{p^\alpha} \in \{0, 1, 2, \cdots\cdots, p^{\alpha-1}\}$. For that purpose express integer x to the base p (instead of decimal 10) by writing

$$x = x_0 + x_1 p + x_2 p^2 + \cdots\cdots + x_{\alpha-1} p^{\alpha-1} \tag{10.16}$$

where $0 \le x_i < p$, and $p^\alpha = 0 \pmod{p}$. Therefore,

$$b\,p^{\alpha-1} = (a^{x})p^{\alpha-1}$$
$$= \left(a^{x_0+x_1p+x_2p^2+\cdots\cdots+x_{\alpha-1}p^{\alpha-1}}\right)^{p^{\alpha-1}}$$
$$= a^{x_0p^{\alpha-1}} \cdot \left(a^{p^{\alpha}}\right)^{x_1+x_2p+\cdots\cdots+x_{\alpha-1}p^{\alpha-2}}$$
$$\equiv a^{x_0p^{\alpha-1}} \cdot 1 \pmod{p} \quad [\text{as } p^{\alpha} \equiv 0 \pmod{p}]$$

and so,
$$\left(a^{p^{\alpha-1}}\right)^{x_0} \equiv b^{p^{\alpha-1}} \pmod{p} \tag{10.17}$$

Similarly,
$$b^{p^{\alpha-2}} \equiv a^{x_0p^{\alpha-2}} \cdot a^{x_1p^{\alpha-1}} \pmod{p}$$

or,
$$\left(a^{p^{\alpha-1}}\right)^{x_1} \equiv (b \cdot a^{-x_0})^{p^{\alpha-2}} \pmod{p} \tag{10.18}$$

and in general,
$$\left(a^{p^{\alpha-1}}\right)^{x_i} \equiv \left(b \cdot a^{-x_0-x_1p-\cdots\cdots-x_{l-1}p^{l-1}}\right)^{p^{\alpha-i-1}} \pmod{p} \tag{10.19}$$

The iterations $x_0, x_1, x_2 \cdots\cdots x_{\alpha-1}$ may be determined by Shank's baby - step giant - step method, determining x given by Eq. (10.16) in modulus p.

ELLIPTIC CURVES IN REAL DOMAIN

The number theoretic applications of elliptic curves have far reaching consequences like the historic proof of *Fermat's Last Theorem* by Andrew Wiles in 1995. It provides a powerful tool in Cryptography. The genesis of the study of these curves lies in the development of the elliptic function $\wp(z)$ by KarlWeierstrass as the solution of the differential equation

$$\wp'(z) = z3 + az + b \tag{11.1}$$

in the complex domain. Instead of dwelling in that subject, there arises the study of *Elliptic Curves* in the $real(x, y)$ domain as the solution of the algebraic equation

$$E(a, b) : y2 = x3 + ax + b \tag{11.2}$$

From the Theory of Equations, if $4a^3 + 27b^2 > 0$, only one of the zeros of the cubic on the right-hand side of Eq. (11.2) is *real*, and the curve has a symmetrical form as shown in figure 1.

In order to construct an algebra of points $P(x, y)$, the coordinates are viewed as a paired number associated with E. For such formalism, it is at first convenient to express the equation of E in *homogeneous coordinates* $(X;\ Y\ ;\ Z)$ in the form

$$E(a, b)\ \ Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{11.3}$$

Figure 1

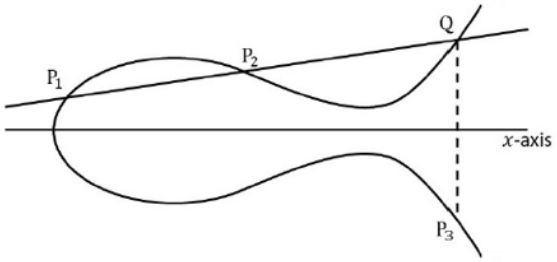

Figure 1 Elliptic Curve form

so that $X/Z = x$ and $Y/Z = y$. This form of the equation has the advantage that the point at infinity is also taken in to account. For that point $Z = 0$ and so $X = 0$ from Eq. (11.3) The arbitrary value of Y is chosen as 1 to set the coordinates of the point as $(0;\ 1;\ 0)$. The other points in the finite domain are $(x;\ y;\ 1)$. The points therefore form the set

$$E(a,b) : \{(x;\ y;\ 1) :\ y^2 = x^3 + ax + b\} \cup \{(0;\ 1;\ 0)\} \tag{11.4}$$

For brevity $(x;\ y;\ 1)$ will be written as (x, y) and $(0;\ 1;\ 0)$ as $\mathcal{O}$.

The algebra of points (or number pairs) on the elliptic curve is developed in the following manner. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the curve. Their sum $P_1 + P_2$ is defined as the reflection $P_3 = (x_3, y_3)$ of the point of intersection Q of the chord joining P_1 and P_2. Let the equation of the chord be $y = \lambda x + \mu$; then since it passes through $P_1 = (x_1, y_1), \mu = y_1 - \lambda x_1$ in which λ is the slope of the chord viz.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ if } P_1 \neq P_2 \tag{11.5}$$

In the particular case $P_2 = P_1, \lambda$ equals dy/dx at the point $P_1 = (x_1, y_1)$, Hence from Eq. (11.2)

$$2y\frac{dy}{dx} = 3x^2 + a$$

or,
$$\frac{dy}{dx} = \frac{3x^2 + a}{2y}$$

and therefore

$$\lambda = \frac{3x_1^2 + a}{2y_1} \text{ if } P_1 = P_2 \tag{11.6}$$

In order to find the coordinates of Q, substituting $y = \lambda x + \mu$ in Eq. (11.2)

$$(\lambda x + \mu)^2 = x^3 + ax + b$$

or,
$$x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + b - \mu^2 = 0$$

whose roots are x_1, x_2 and x_3. Hence,

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2) = (x - x_1)(x - x_2)(x - x_3)$$

$$= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x - x_1x_2x_3$$

Equating the coefficients of x^2 on the two sides of the above identity

$$\lambda^2 = x_1 + x_2 + x_3$$

or,
$$x_3 = \lambda^2 - x_1 - x_2 \tag{11.7}$$

Eq. (11.7) gives the value of x_3. The value of y_3, keeping in mind the reflection of Q about the x-axis leads to

$$-y_3 = \lambda x_3 + \mu = \lambda x_3 + y_1 - \lambda x_1$$

or, $$y_3 = \lambda(x_3 - x_1) - y_1 \quad (11.8)$$

which yields the value of y_3.

In the above construct, if $x_2 = x_1$ and $y_2 = -y_1$, then according to Eq. (11.6), the chord is parallel to the y-axis and P_3 is a point at infinity, that is $P_3 = \mathcal{O}$. In this case $P_1 + P_2 = \mathcal{O}$, which is rewritten as $P_2 = -P_1$. This means that since $P_1 = (x_1, y_1), -P_1 = (x_1, -y_1)$, and $P_1 + (-P_1) = 0$. Thus $\mathcal{O}$ acts like zero for elliptic curves and so $P_1 + \mathcal{O} = P_1 = \mathcal{O} + P_1$.

FINITE FIELD ELLIPTIC CURVES

The algebraic construct of the elliptic curves in the domain of real numbers can be restricted to a finite field $\mathbb{F}_p$ of integers by considering only the points belonging to such restricted set of numbers in which addition is interpreted as a modulo p sum. Thus, an elliptic curve on the *prime field* $\mathbb{F}_p$ is the set

$$E(p;\ a, b) = \{(x, y) :\ y^2 = x^3 + ax\ +\ b\} \cup \{\mathcal{O}\} \quad (11.9)$$

with the algebraic properties that

(i) $P + \mathcal{O} = \mathcal{O} + P = P$ for $P = (x, y)$

(ii) $P + (-P) = \mathcal{O}$ for $P = (x, y)$ and $-P = (x, -y)$

(iii) If $P_1 = (x_1, y_1)$ and $P_3 = (x_3, y_3)$, then,

$$P_1 + P_2 = (x_3, y_3)$$

where $x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda\ (x_3 - x_1) - y_1$, and

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{for } P_1 \neq P_2 \\ \dfrac{3x_1^2 + a}{2y_1} & \text{for } P_1 = P_2 \end{cases}$$

It can also be shown that the addition law is a associative, that is $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$. The proof of this property is intricate and omitted here.

Example. Find the set of points in $\mathbb{F}_p$ of $E(7;\ 3, 2) :\ y2 = x3 + 3x + 2$.

The points can be found by setting $x = 0, 1, 2, 3, 4, 5, 6$ and checking for which values the quantity $x^3 + 3x + 2$ is a square modulo 7.

For $x = 0, y^2 = 2$, which has no $\pmod 7$ solution.

For $x = 1, y^2 = 6$, which has no $\pmod 7$ solution.

For $x = 2, y^2 = 16$, and $42 \equiv 16 \pmod 7$.

For $x = 3, y^2 = 38$, which has no $\pmod 7$ solution.

For $x = 4, y^2 = 78$, and $62 = 36 = 78 - 6 \cdot 7 \equiv 78 \pmod 7$.

Proceeding in this manner, for $x = 5$ and 6 there is no solution. Hence,

$$E(7;\ 2, 3) = \{\mathcal{O}, (2, 4), (4, 6)\}$$

In general, it is clear that the set of points $E(p;\ a, b)$ is finite, since there can only be finitely many possibilities for the x and y. To be precise, there are p possibilities for x and then for each value of x, the equation of the elliptic curve can yield only two possibilities for y. Adding the extra point $\mathcal{O}$, the number of points $\#E(p;\ a, b)$ can at most be $2p + 1$. A tighter limit is however given by Hasse's theorem according to which

$$\#E(p;\ a, b) = p + 1 - t_p \quad (11.10)$$

where $|t_p| \leq 2\sqrt{p}$. The proof of this theorem is also omitted here because of further technicalities involved.

It can be foreseen that the complicated way of deciphering the number pairs of an elliptic curve in prime field $\mathbb{F}_p$ makes it eminently suitable for Cryptography.

CONCLUSION

Cryptographic methods for securing digital data is heavily dependent on some Number Theoretic results. This survey article presents the essentials of this algebraic topic in a simple, clear manner, in aid of studying the subject of Cryptography. In summary, the algebra of congruences, prime numbers and several theorems related to them are covered. These topics include, representation of the division algorithm as a congruence, Euclid's algorithm for calculating *GCD*, properties of prime numbers leading to the theorems of Fermat and Euler, developing the properties of the latter's phi function, linear congruences and the Chinese remainder theorem; primality tests, factorisation of composite numbers and discrete logarithms. Finally, a description of the elliptic curve prime field is presented, which has lately come in to prominence. A quick study of this survey, it is hoped will be a useful aid for a prospective reader of the subject of Cryptography.

ACKNOWLEDGMENTS

The author is sincerely thankful to Ajijul Hoque, Department of Mathematics, IIT Kharagpur for helping preparation of this article.

DECLARATIONS

There are no conflicts of interest in the research reported in this paper. And no data were generated or analysed by AI or otherwise in the presented research.

REFERENCES

Bernard, S., and Child, G. M. (1965). Higher Algebra. Macmillan.
Buchmann, J. A. (2002). Introduction to Cryptography. Springer. https://doi.org/10.1007/978-1-4684-0496-8
Chrystal, G. (1906). Algebra: An Elementary Text-Book, Part II. Adam and Charles Black.
Dietzfellinger, M. (2004). Primality Testing in Polynomial Time (Lecture Notes in Computer Science, Vol. 3000). Springer-Verlag. https://doi.org/10.1007/b12334
Hardy, G. H., and Wright, E. M. (1938). An Introduction to the Theory of Numbers. Clarendon Press.
Hoffstein, J., Pipher, J., and Silverman, J. H. (2008). An Introduction to Mathematical Cryptography. Springer.
McAndrew, A. (2011). Introduction to Cryptography with Open Source Software. CRC Press.
Niven, I., Zuckerman, H. S., and Montgomery, H. L. (1991). An Introduction to the Theory of numbers. John Wiley and Sons.
Paar, C., and Pelzl, J. (2010). Understanding Cryptography. Springer. https://doi.org/10.1007/978-3-642-04101-3
Rosen, K. H. (2005). Elementary Number Theory and its Applications. Pearson/Addison Wesley.